Automating Malware Analysis for Proactive Detection

Paul Melson

Why Do We Analyze Malware?

Props for Viper

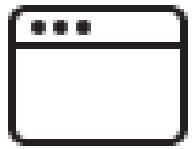
- Claudio Guarnieri (@botherder)
- Alexander Jaeger (@alexanderjaeger)
- Kevin Breen (@kevthehermit)
- Raphael Vinot (@raphi0t)
- 24 other really awesome people!

Viper Overview

- Repository and framework for static file analysis
- Python, SQLite
- Interfaces:
  - Command Line
  - Web
  - API
- Open module template

presentation

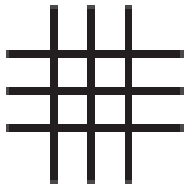
web UI



CLI

software

api



framework

modules

infrastructure

database

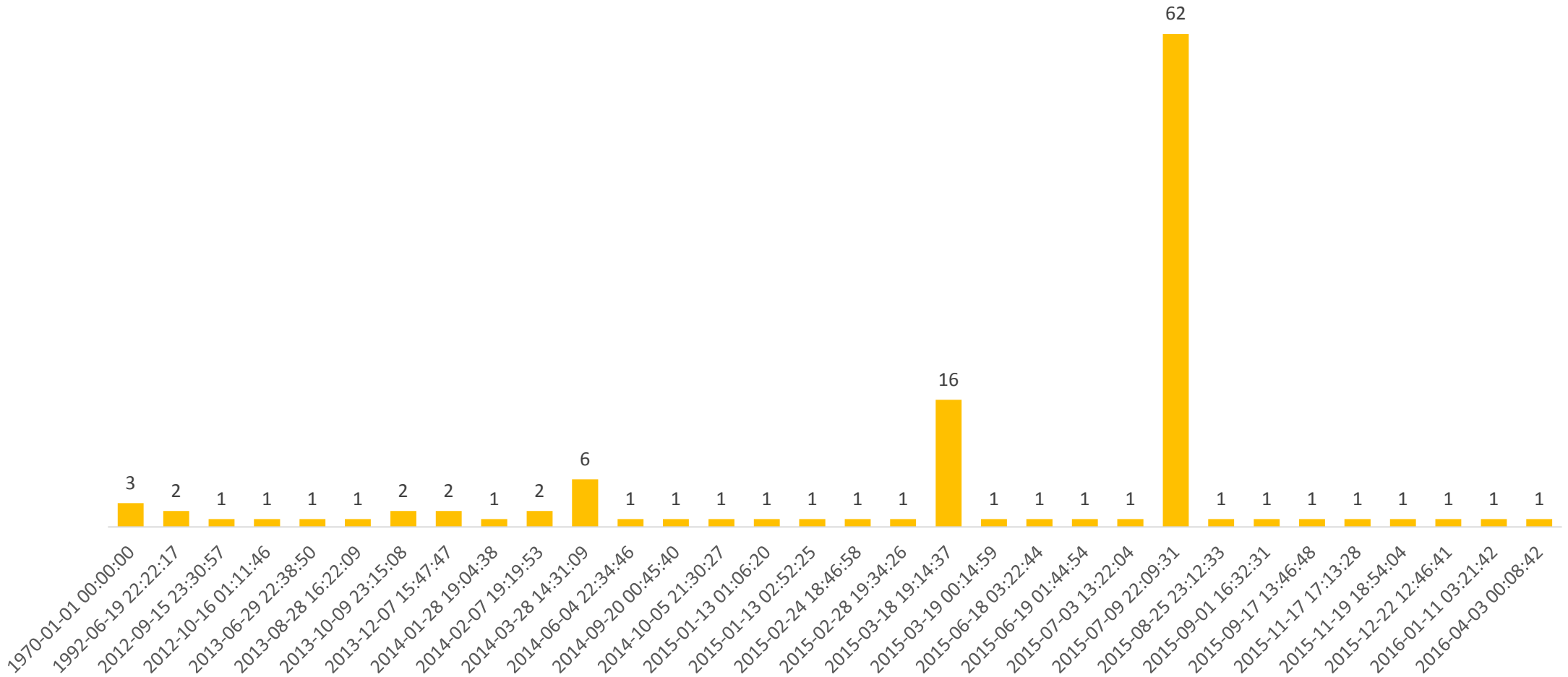
file structure

“The Zoo” Use Case

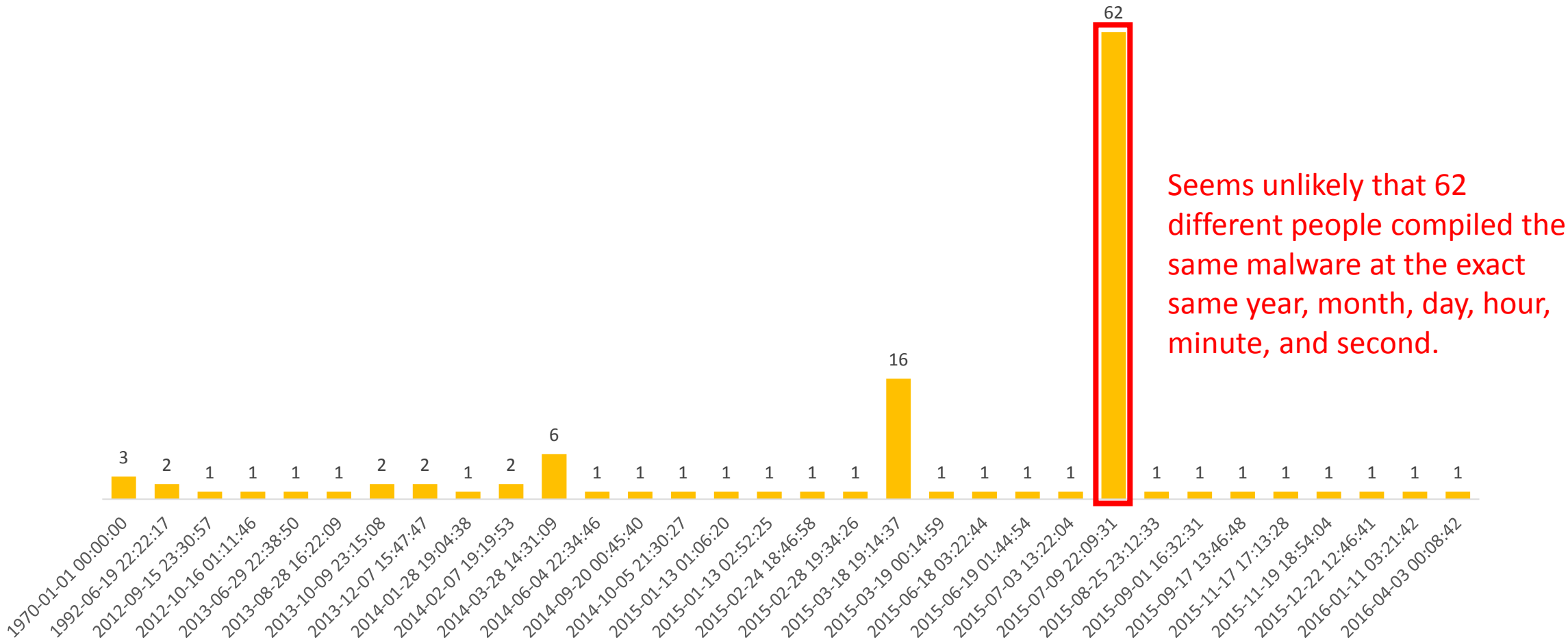
- Historical Evidence
- Threat/Attacker Intelligence
- Analysis & Data Mining

Time for some live demos!

PE Compiletime Groupings



PE Compiletime Groupings



Seems unlikely that 62 different people compiled the same malware at the exact same year, month, day, hour, minute, and second.

More Live Demos!

Let’s Talk!

https://github.com/pmelson